Adrian Gregory
Chair, IDM Data Council, Chief Executive, DQM Group. Gregory has over 25 years of experience in data working across B2C and B2C in marketing and location-based services' applications. His current organization DQM Group, formed in 1996, has grown to become the most trusted independent provider of Data Governance services to the UK marketing industry, working for over 80 per cent of leading commercial data owners and increasingly leading brands. DQM Group has won numerous industry awards including Data Strategy, Data Service Provider of the Year for 2007, 2008 and 2009. In addition to his role at DQM Group where he spends 50 per cent of his time on strategic data assignments for customers, he is Chairman of the IDM Data Council and the DMA Data Governance Working Party.

Lisa Bentall
Chief Data Risk Officer, Director DQM Group. Bentall has over 25 years of experience in data and compliance management. A founding partner of DQM Group, she specializes in helping clients identify and control the risks associated with managing valuable data sets. She heads DQM's team of information security, regulatory compliance and governance auditors, and is an ISMS Lead Auditor and Member of the IAPP.

Keywords: Data governance, third-party processors, risk, security, management process

Adrian Gregory
DQM Group Limited
DQM House
Baker Street
High Wycombe
Bucks HP11 2RX
UK
Tel: 440 870 242 7788
E-mail: adrian.gregory@dqmgroup.com

Data governance — Protecting and managing the value of your customer data assets

Stage 3: Identifying and controlling the risk in using third-party processors

Adrian Gregory and Lisa Bentall

Received (in revised form): 13th February 2012

Abstract

In a previous edition of the IDM's *Journal of Direct, Data and Digital Marketing Practice*, we made the case for investing in your customer data and outlined an effective approach for improving the quality of data over the long term. With the case for treating customer data as a key business asset made in the first two papers, this third and final paper focuses on how organizations of any size can significantly reduce their risks and exposure when using third parties to process their data. It focuses on identifying third-party touch points and putting simple but effective risk management controls in place. *Journal of Direct, Data and Digital Marketing Practice* (2012) **13,** 335–344. doi:10.1057/dddmp.2012.5

The need for this paper — Introduction

The Data Protection Act (DPA) defines two categories of organization involved in the handling of personal data: data controllers, who decide what to do with the data, and data processors who process the data on behalf of the data controller. Data processors have no statutory responsibilities or obligations — all responsibility rests with the data controller.

The Seventh Principle of the Act states that where you use a data processor, you must

- choose a data processor that provides adequate guarantees of its security measures to protect the processing it will do for you;
- take reasonable steps to ensure that those security measures are being put into practice;
- have in place a written contract setting out what the data processor is allowed to do with the personal data. This contract must also require the data processor to take the same security measures you would have to take if you were processing the data yourself.

If the data processor loses your data, the Information Commissioner will hold you responsible for any breach of security or loss of personal data, not the data processor. You may take action against the data processor for breach of contract, but they may not have sufficient insurance for you to recover the substantial fine you have paid — and it is unlikely that they can compensate you adequately for the bad publicity and loss of revenue engendered by the data breach. This paper sets out the key steps you can take to prevent a data processor breach and to meet your DPA obligations.

Quantifying the risk

'£29 lost business for each individual record lost'

Let us start with the basics — What is the cost?

Any data breach has the potential to cause a significant loss of customer trust, loyalty and revenue. Research from the Ponemon Institute in 2010 shows that there is an average 3.9 per cent customer churn following any data breach and an average of £29 lost business for *each individual record lost*.

Then there is the considerable cost in addressing the immediate problem. You may already have a Data Breach Notification Plan in place to guide you through the complex process of advising customers and statutory bodies. Notification of the Information Commissioner is voluntary in the United Kingdom — although with a strong expectation that public sector organizations will notify — but is mandatory in many other countries. The requirements of implementing this plan — the notification process itself, seeking professional advice, advice notices to customers, help lines to answer queries, briefings to customer facing staff, additional PR, staff time taken to address and control the issue — bring the cost per compromised record to an estimated £130.

Finally, there is the cost of any regulatory penalty. From January 2010, the Information Commissioner has had the power to levy fines of up to £500,000 for breaches of the DPA. In November 2010, government and local authority contractor A4e became the first organization to be fined under the ICO's new powers. The company was fined £60,000 following the theft of an unencrypted laptop containing details of 24,000 Hull and Leicester community law centre customers from an employee's home.

'What's the ROI for compliance?'

According to the first benchmark study to estimate the costs associated with an organization's compliance efforts — conducted by Tripwire and the Ponemon Institute last year — dedicated investments in compliance activities are not only a critical component of a comprehensive enterprise security strategy, but can also offer return on investment over time. *The average cost of non-compliance was found to be 2.68 times higher than compliance costs*.

'Four key risks'

What can go wrong?

There are *four key risks*:

1. Your data may be lost accidentally by the data processor.
2. Your data may be deliberately targeted and stolen from the third party's site.
3. The third party may compromise your compliance with the DPA or other regulations through careless or inappropriate use of your data.
4. The quality and accuracy of your data may be compromised by poor third-party processes.

Case study: Zurich insurance and accidental loss

In 2010, Zurich Insurance was fined a record £2.27m by the FSA for the loss of 46,000 customer records.

Zurich had outsourced the processing of some of its customer data to a Zurich group company in South Africa. In August 2008, Zurich SA lost an unencrypted back-up tape of these data during a routine transfer to a data storage centre. Because it did not have adequate reporting lines in place, Zurich UK did not even learn of the incident until a year later. The FSA concluded that the company 'failed to … ensure it had effective systems and controls to manage the risks relating to the security of customer data resulting from the outsourcing arrangement'.

What steps can you take to control these risks?

Step 1. Map your data flows and touch points

'Understand what data go where'

Identify what data you hold — establishing the location and accesses permitted to all the caches of data throughout the organization can in itself be a revealing and valuable exercise.

Next, who has access to your on-site data? Which employees, in which areas of the organization? Are data also distributed to branches, franchises or other group companies? What scope does each of these internal users have to pass data on to external third parties, and what controls are in place?

Are third parties involved in inputting data? For example, do you use third-party online service providers or call centres to collect data? Do you purchase data from third parties or take part in a data pool? If so, you need to ensure that third parties collect data compliantly, efficiently and with appropriate permissions. There is no point in collecting and inputting customer information that you do not have the right to use.

Next, who do you send data to for business services? Do you use different call centres for outbound calling? What computer bureaux, printers and mailing houses do you use? Do you use external email marketing or analytics? What levels of confidence do you have in their security and controls?

And finally any others — for example, previously contracted third parties with whom you no longer have a relationship but who might still hold historical data or perhaps worse still have access.

Case study: ACS: Law and the DPA

Earlier this year, ACS: Law's website was hacked and confidential details of BT and Sky customers were downloaded and published on the internet. ACS was targeted because it has sent thousands of letters to individuals suspected of illegal file sharing, but the ICO has made it clear that the fact that the security breach resulted from a deliberate attack is not a sufficient defence.

Case study: Call centres and deliberate theft

In 2007, Strathclyde Police reported that one in ten Glasgow call centres had been infiltrated by criminal gangs, who either suborned existing employees or actively sought employment in order to gain confidential financial data.

Identifying all the third parties who have access or potential access to your data can be a disconcerting process. Royal Bank of Scotland (RBS) recently audited the activities of over 850 third parties around the world — an extended network ranging from bank statement printers to computer hardware providers, from publishers and payroll processors to cash logistics firms and lawyers.

Step 2: Set internal rules and standards

Once you have a clear picture of how data are used and who currently has access to the data, the next step is to establish internal rules for the provision of data to third parties. As a minimum, this process should consider:

'Good data governance starts with data minimisation'

- How each third party is managed and by whom. Someone must be responsible for managing the third-party relationship throughout its lifetime and for ensuring that appropriate contracts and Service Level Agreements (SLAs) are in place.
- Minimum terms for these contracts and SLAs that are consistent across all third-party relationships.
- The objective of supplying the data to a third party. Be very clear internally and with each third party about why the data are being supplied and how the third party is permitted to use the data.
- How much data will be released. Provide each third party with the minimum depth and volume of data required to achieve their objectives. Good data governance starts with minimization — ensuring that as little data as possible are provided to as few people as possible, for as little time as possible.
- How the data will be provided. The distribution method should reflect the volume and sensitivity of the data in transit — and should mandate how the data will be returned.
- How you will monitor third-party use of your data.

Step 3: Set consistent rules for third parties

The next step is to ensure that your expectations and requirements are fully understood and agreed across all your third parties via contracts and SLAs.

Contracts should stipulate:

- That you expect third parties to comply with the DPA, Privacy in Electronic Communications Regulations and any other applicable legislation — although remember that the buck stops with the data controller not the processor.
- That you have the right to audit third-party activities and to use data seeding to monitor use.
- Termination clauses — what will happen to your data when the contract is terminated?
- SLAs — which detail the rules and requirements relating to the people, processes and technology used in delivering the service.

Approximately 80 per cent of data breaches are down to user error, and thus having your third parties' commitment to adequate control of people is a vital element of governance.

Case study: Skipton and data corruption

In January 2010, Skipton Building Society was forced to apologize to customers after a breach of data security procedures resulted in thousands of savers receiving financial details about other customers in an account statement mailing. The building society said a third-party printing error led to the account details of 3,115 customers being printed on the back of other people's statements. The ICO again took a dim view, stating 'Even when the breach occurs as a result of third parties processing personal information, the data controller … should ensure the necessary security policies and procedures are in place and that all employees are made aware of them'.

'Creating a robust SLA'

What the SLA should cover

The SLA should be agreed with and signed by the third party and should include the following:

- The names or as a minimum the roles of the individuals that will have access to your data. You might wish to stipulate that temporary or contract staff may not have access without your express permission in writing.
- That any change of personnel must be communicated to you within an agreed timeframe.
- The kind of training and security awareness these employees will receive with regard to your data and how often this is repeated.
- That the number of individuals who have access to your data will be strictly limited and that access will be solely to achieve your business objectives. Consider too how access rights are withdrawn when someone leaves or changes role.
- Mandate that your third parties' data operating procedures and processes around your data are documented. This serves two key functions: you can confirm that they understand your instructions,

plus you'll be more confident that those instructions are passed on to the third-party delivery team correctly.

- Agree on the number of copies of your data they are permitted to make and, very importantly, how long these may be retained. If copies proliferate unchecked, returning or deleting them at the end of the contract may prove impossible to manage effectively.
- That data no longer required should be clearly marked and returned to you or securely destroyed. The third party should be able to account for every copy or version of your data at periodic intervals or on contract termination.
- Restrict any further outsourcing of activity by your chosen third party, or at the very least require that your permission be given for any further third party usage. Your terms and conditions, both contractual and within the SLA, should be passed on down the chain.
- The technical security controls in line with your organization's own security practices. Including;
  - physical and environmental security controls such as restricting access to the areas where your data are held;
  - the use of controls such as firewalls and anti-virus protection;
  - how the restrictions on who can access your data are implemented and the robustness of this process, including what kind of access logs are in place, how long they are retained and how often they are reviewed for unauthorized activity.
  - how many back-ups the third party is allowed or required to take and at what intervals, both for business continuity reasons and for good data governance.
- Consider also what will happen in the event of contract termination. In certain instances, you may mandate that your data must be backed up and retained separately from any other data held by the third party.

Check that they play by the rules

Conduct regular audits and agree remedy plans

All contracts with third parties should give you the *right of audit*. The audit serves two functions, enabling you to check the performance of data processors *and to demonstrate that you have done so*. You should use the audit to check that their care and use of the data corresponds to the contract and SLA. In a perfect world, you would audit all third parties at the start of the working relationship and then on a regular basis, for example annually, although this will vary according to the volume and complexity of third-party relationships that your organization might have and the resources you have available.

Where complete coverage is unachievable, aim to focus your resources on those third parties that pose the greatest risk — those who have access to the most sensitive or valuable data, those where you have had problems in the past, or those with whom you work most frequently.

'Testing compliance'

Audit objectives are not punitive but simply to ensure that issues are identified and fixed within an agreed timescale — although in the event of consistent or major failure to meet the agreed standards you may choose to move your valuable asset to a more reliable suppler.

The audit should look at the key controls defined in the contract and the SLA and check that they have been implemented and are operating effectively. Ask to see proof — documented operating procedures, training records, recruitment checks and employment contracts. Talk to the individuals who work on your contract and ask them about their understanding of data protection and data security. If the company tells you that all employees receive training in the organization's Acceptable Use Policy, for example, ask different individuals about aspects of this policy. Are they allowed to work on your data at home? Are they allowed to share passwords when accessing your data?

Where issues are identified during an audit, you need to agree on a remedy plan with your supplier including the specific changes they will make and the timescale in which these changes must be completed. You could choose to revisit to ensure that these changes have been made or look for some documented evidence.

Seed your data

'Using seeds to identify misuse'

To underpin this audit programme, you should also seed your data. Seeding is the process of adding dummy names with real contact details such as address and telephone number to data and is the way data owners generally keep track of what their customers are doing. In principle, it is an easy way to monitor end users and compare their activity against licence terms.

However, seeding has other applications and can be a powerful tool in monitoring the activities of data processors. Seeding can provide an early warning of any theft of your data — for example, if the seed names receive renewal calls from another company prior to the end of a mobile telephone contract, or if they receive marketing emails from organizations other than your own or any trusted and vetted partner companies. Seeding also provides you with confirmation that your campaigns are being executed properly — mailings or emails sent on time, correct packs to correct cells for example. Last but by no means least, seeding provides proof of misuse, giving you the opportunity to enforce compliance or even prosecute if necessary. Rosemary Smith, director at Opt-4, talks about seeding as 'a no-brainer. Years ago, I had a case taken to court on the basis of seed names showing misuse. They settled out of court for a significant amount of money. When we went to get advice from counsel, those seeds were seen as absolute proof'.

Seeding does not have to be a complex or expensive process to be successful. Lynn Stevens, Managing Director of Lloyd James, describes the organization's seeding programme as 'based on a simple system of friends and family around the country. We add seeds to data using unique initials each time. It is part of our process, not something we discuss at the start. We are trying to control what happens and control how people are using the information'.

Publicize your use of seeds and describe it in your contracts, ensuring that third parties understand that the data are being monitored.

Outsourcing third-party controls

The steps listed above, from mapping your touch points to auditing and seeding third-party activity, all relate to the robustness of your policies and processes and can all be undertaken internally using existing resources. A keen appreciation of where your key risks lie and the will to make your data more secure are more important than a specialist skill set.

'Complex and large-scale third-party usage'

However, there are some organizations for which it is obvious that data management rapidly escalates into a complex process. With a long supply chain across and beyond the enterprise, the challenge of maintaining the completeness, integrity and availability of data is clearly growing. Data governance structures and the need to demonstrate compliance mean each point of data entry, usage and transfer needs to be closely controlled, monitored and audited. As a result, an organization may choose to outsource some or all aspects of third-party control. While at first sight this may appear to be at variance with the goal of risk management and control, it has the significant benefit of allowing the company to focus its resources on managing a limited number of relationships and managing those relationships well.

In 2010, KPMG with RBS won the Business Strategy category at the MCA Management Awards for a full-scale data security review of all of RBS third-party relationships. Worried about the risk of data loss among the bewildering array of third parties with which it had dealings, RBS commissioned KPMG to identify each of the third parties with which it shared data, audit the information security of each supplier and recommend changes where appropriate. KPMG audited a staggering total of 860 suppliers over a 13-week period and has now implemented a standard process across RBS for reviews and assessments of new and existing third parties.

'Automating elements of governance and management'

In 2011, DQM Group launched its Secure Distribution Hub, a suite of services and solutions that link up multiple data management stages, apply the appropriate inputs and provide management information (Figure 1).

Early adopters of the Hub are data owners who see the service as a straightforward and cost-effective means of ensuring that they meet their data protection obligations and receive all the revenues due to them. Royal Mail adopted this system to ensure their business is operating and benefiting as planned from the multiple data sets the organization releases through third-party resellers.

However, the Secure Data Hub should prove equally valuable to any organization needing to track which data processors have received data and to check how those data are being used.

The distribution module comes into play where data are licensed to multiple different end users, each taking a specific cut or profile of the records, and where different data sets are provided to multiple

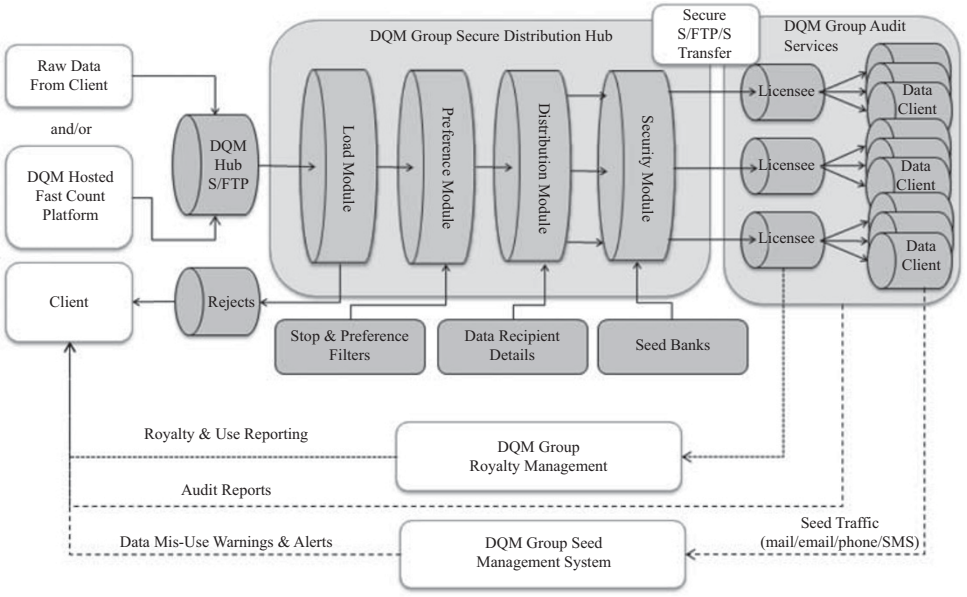

Figure 1: Automating elements of governance and management

third-party data processors. The configuration for each version of the file is pre-set in this module to ensure they receive data exactly as they are expecting it — and to ensure that the organization's internal rules as to what data can be provided to which third-party processor are adhered to.

Seeding is then applied. The templates created for the load module play an important role here because they ensure that seed records appear in the file looking exactly like the original records. This also applies to any specific selections, and thus if data need to meet a set geography, only seeds from within that region will appear. The number of seeds added at this stage is also proportionate to the file size.

Conclusion

As the Data Controller, it is your responsibility to control the use of the personal data you hold and the Information Commissioner has been shown to have little sympathy with organizations that abdicate responsibility to unreliable and untested third parties. Introducing robust internal processes around who can dispatch data to external organizations and what data can be sent will go some way towards resolving this issue; implementing standard contract clauses and tough SLAs for third parties will take you even further. Above all, protecting the value of data assets released to third-party processors is about actively managing those relationships and continually checking that your standards have been met and your data remain protected.

Summary key points

In this paper, you will have learned:

- The reasons why it is vital to police your relationships with third-party data processors in order to meet your obligations under the Data Processing Act;
- The key risks posed by these third-party relationships;
- The importance of creating consistent internal rules for who can supply data to third parties and what those rules should cover;
- How to manage the data processor relationship through contracts and SLAs;
- What the SLA should contain;
- How to monitor and improve data processor compliance through seeding and auditing.

References and Notes

1. http://www.forrester.com/rb/Research/calculating_cost_of_security_breach/q/id/42082/t/2.
2. http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2010%20Global%20CODB.pdf.
3. http://www.computerworlduk.com/news/security/3442/tk-maxx-data-breach-costs-could-hit-800m/.
4. http://mike2.openmethodology.org/wiki/What_is_MIKE2.0.
5. http://www.datameasures.com.
6. http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2010%20Global%20CODB.pdf.
7. The Economist. (2010), Data, data everywhere. A Special Report on managing information. *The Economist* February.
8. DQM Group. (2010), 'Turn Your Customer Data into a Strategic Business Asset — A Directors' Briefing.
9. The DGI Data Governance Framework. Gwen Thomas, The Data Governance Institute.
10. Governance, Risk and Compliance Series — The Role of Data Governance in GRC. Mike Ferguson, Intelligent Business Strategies. July 2010.
11. Governance, Risk and Compliance Series — the Role of Data Governance in Mitigating Risk. Mike Ferguson, Intelligent Business Strategies. August 2010.
12. Tony Fisher. (2009), The Data Asset. How Smart Companies Govern their Data for Business Success.
13. Adelman, S., Moss, L. and Abai, M. (2005) 'Data strategy'.
14. Dyche, J. and Levy, E. (2006) 'Customer data integration', *Reaching a Single Version of the Truth*.
15. English, L.P. (2009) 'Information quality applied', *Best Practices for Improving Business Information Processes*.
16. DQM Group. (2010) 'Customer data — The threat from within — A directors' briefing.
17. Crosby, P.B. and Penguin Group (1979) 'Quality is free'.
18. Redman, T.C. (2001) *Data Quality, The Field Book*, Digital Press.
19. McGilvray, D (2008) *Executing Data Quality Projects*, Elsevier.